Air Live®
Powered by OvisLink Corp.

MW-2000S

Wireless Security Gateway

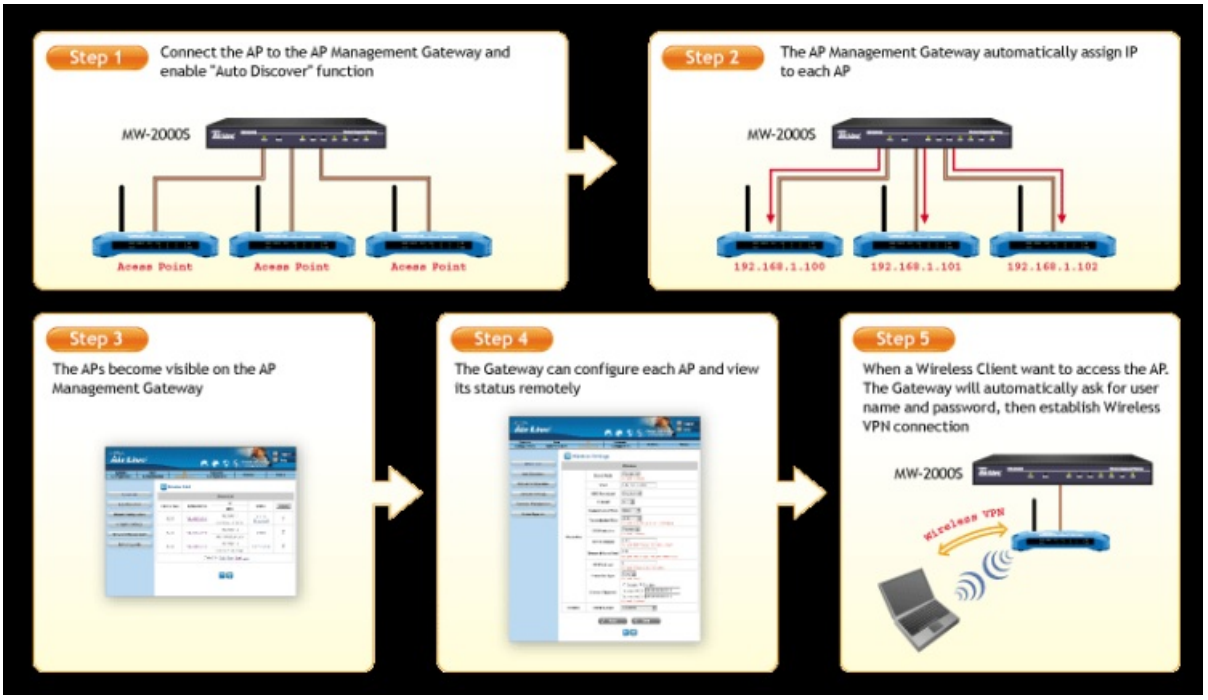
Is your office still not using wireless LAN because of the concern for security? If it is, then your concern is legitimate. Since the regular WLAN network must use the same encryption key, once the encryption key is given, you are risking exposing your network to outsider. What's even worse is that when you need to change encryption key, you must change it on all the AP and notify all the users. What you need is the MW-2000S. It takes care of all your concerns and much more...

Problems Faced by Enterprise Wireless Deployment			
Problem	Unable to Centrally Managed Access Points	Unable to Effectively Protect and Encrypt Wireless Data	Unable to Password Protect Intranet and Internet Access
Explanation	If an AP goes down, the administrator does not notice immediately. Any Changes to the wireless setup involves changing settings on all the APs and clients.	If the Encryption Key is known to one user, the network is exposed to risk All access point must be set to the same WEP or WPA Encryption	Password Protection must be Web or Email Activate for easy to use In addition, we must have different account types and usage control for different users.
The Solution	**AP Management**	**Wireless VPN**	**Authentication Gateway**

3 Security Servers in One

The MW-2000S is a complete wireless security solution that include 3 security servers in one box. Working together with our WL-5460AP wireless Access Point, it provides an easy-to-use yet extremely powerful solution for office wireless deployment. Its installation is extremely simple in 5 easy steps.

Manufacturer
OvisLink Corp.
2F, No. 8, Lane 130, Min-Chuan Rd, Hsin-Tien City, Taipei, Taiwan.


Step 1
Connect the AP to the AP Management Gateway and enable "Auto Discover" function
MW-2000S
Access Point
Access Point
Access Point
Step 2
The AP Management Gateway automatically assign IP to each AP
MW-2000S
192.168.1.100
192.168.1.101
192.168.1.102
Step 3
The APs become visible on the AP Management Gateway
Step 4
The Gateway can configure each AP and view its status remotely
Step 5
When a Wireless Client want to access the AP. The Gateway will automatically ask for user name and password, then establish Wireless VPN connection
MW-2000S
Wireless VPN

AP Management

The MW-2000S can manage up to 12 x WL-5460AP 802.11g wireless access points. Comparing to competitor's product that require using expensive dedicated AP, the WL-5460AP is a powerful multifunction AP with 7-mode functions at amazing affordable price. The MW-2000S AP Management comes the following powerful functions

Auto AP Discovery:
- Keep your AP in the factory default configuration, and connect it to the MW-2000S. Then press "Auto Discover" and the MW-2000S will find all the APs for you

Auto IP Assignment::
- The MW-2000S will assign different IP to each AP automatically.

Template Configuration:
- You can define default configurations for the AP in a template file. So after AP is discovered by the security gateway, you can assign the configuration template to each AP. You no longer have to configure each AP independently.
- Up to 3 configuration templates can be defined.

Viewing AP Status::
- View the wireless and LAN status
- Disable or Enable each AP

Detail Configuration:
- Configure all the AP's function from the MW-2000S web interface

Uniform Firmware Upgrade:
- pload the AP's firmware to MW-2000S, then the MW-2000S will upgrade all your AP's firmware.

Keep Alive Status:
- Up to 40 IP addresses can be set in the Keep Alive status function. So when one network device is down, the administrator would receive email about this.

Air Live®
Powered by OvisLink Corp.

AirLive MW-2000S Advantage		
Model	AirLive MW-2000S	Competition's Product
AP Management	• Using low cost AP solution such as our WL-5460AP • Auto AP Discovery, Auto IP Assignment • Configuration Templates for uniform configuration across all APs • Ability to view Status of individual AP • Able to configure each AP independently • Uniform Firmware Upgrade • Email notification for failed IP	• Use expensive dedicated AP that cost many times more • Has less features than AirLive solution.
Wireless VPN	• Clientless Installation • IPsec security • Auto Key assignment • Complete Transparent to end users	• Not Available on Comparable solutions
Hotspot Authentication	• Guess Account, Instant Account, Permanent Account • Simple to use Instantly generated Account • Set different usage time limit or data limit • Wall Garden feature • Web and Email trigger authentication	• Only simple password authentication
Summary	The AirLive MW-2000S is the only wireless security gateway that combines all 3 security server function at much more affordable cost than previous solutions.	

Wireless VPN

Data encryption means to encode the data so that confidential information can not be stolen by intruder. Since wireless data can be received by anyone with a wireless device, the data encryption is even more important. The current solution require administrator to set wireless encryption key on the wireless device. The problem with this implementation is that when the key is known to one user, the entire network security is in jeopardy. The wireless VPN is the perfect solution to this problem. It is achieved in 5 easy steps.

- **Each user will be give an different account with username and password.**
- **When user try to access the network, a windows will pop up to ask for the account information**
- **WMS Utility:** The WH-9000MESH includes a WMS utility to let administrator manage and monitor all the APs in the MESH network
- **After user enter the correct password, the MW-2000S will download an ActiveX VPN client into the user's PC**
- **The VPN key is automatically assigned, the end user does not need to do anything.**
- **After the account expired, the user will not be able to access the network anymore**

Air Live®
Powered by OvisLink Corp.

Hotspot Authentication

The MW-2000S comes with full featured authentication functions. Therefore, you can manage each user's access time and access right precisely:

Instant Account :

- In the office environment, this type of account is designed for visitors that uses your network on temporarily basis. The administrator first defines account type base upon price, usage time limit, or traffic limit. Up to 10 different account type can be defined. Then when a new account is needed, administrator just select the account type to instantly generate a new account. A new account with username and password is created. Up to 2000 on-demand account can be generated.

Permanent Account :

- For monthly subscriber or permanent PC in the office. The permanent account stay active until disabled. Up to 500 users account can be created.

Web Trigger Authentication:

- When you open the web browser, the MW-2000S will pop up a windows asking you to enter username and password. The pop-up windows can be customized to put your company's logo or art design.

Wall Garden:

- A list of website that unauthenticated users can access. It is a good way to promote your wireless service.

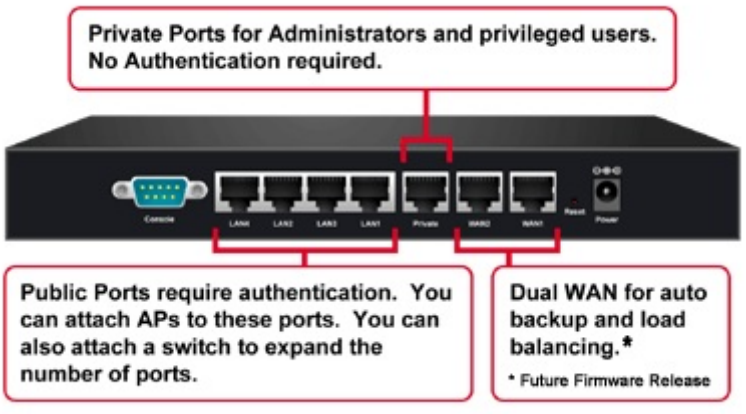
The MW-2000S also comes with 2 WAN ports that will be upgraded for auto backup and load balancing features for the future firmware release. When it comes to enterprise wireless deployment solution, the MW-2000S is your only choice. Don't risk exposing your network to security problems, buy the MW-2000S today.

** Currently, the MW-2000S only work with WL-5460APv2 e5 firmware. Please download the firmware from our website if you do not have the correct firmware installed on WL-5460AP*

*** The ActiveX wireless VPN client only works on WIn2000 and WinXP.*

**** In MW-2000S, the instant guest account can access the Internet only. For Intranet and VPN access, please use regular accounts. You should put the wireless network in the Public ports and the wired network in the public network.*

Ack Panel


Private Ports for Administrators and privileged users. No Authentication required.
Public Ports require authentication. You can attach APs to these ports. You can also attach a switch to expand the number of ports.
Dual WAN for auto backup and load balancing.*
* Future Firmware Release

Air Live®
Powered by OvisLink Corp.

Specification

Features
- Manage up to 12 WL-5460AP
- AP Management with auto discovery
- Wireless VPN
- Hotspot Authentication
- Dual WAN port
- Complete Solution to provide SMB Wireless Service
- 2000 Instant Account, 500 Permanent Accoun5s
- 125 Concurrent Users

Hardware
- CPU: Intel IXP-425, 533Mhz
- Flash: 32 Megabytes
- DRAM: 128 Megabytes
- 1 x N-Type Antenna Connector for Bridge-Mode

Connectors
- 2 WAN Port (10/100 Mbps)
- 1 Private LAN Port (10/100 Mbps)
- 4 Public LAN Port (10/100 Mbps)
- 1 Console/Accessory Port (RJ-11)
- 1 Reset Button
- 1 Power Connector

AP Managment
- Manage up to 12 WL-5460AP
- Auto AP Discovery
- Auto IP assignment
- Failure Notice by Email
- Configuration Templates
- Central Configurations
- AP Status viewing
- AP Disable/Enable
- Assign each wireless port as public (authentication required) or private (no authentication)
- Centralized Firmware Upgrade

Wireless VPN
- Clientless Installation
- Auto Configuration
- No users configuration required
- Configuration Key is invisible to clients
- IPsec Secure VPN Tunnel Encryption works on both wireless and wired connection.

Hotspot Authentication
- Guest Accounts can have different usage time or traffic
- Normal Accounts are permanent accounts for regular office PC and Servers
- Up to 2000 accounts can be created
- Web and Email Triggered login screen
- Customized Login and message screen
- Firewall and Policy to control precisely what user can do

Networking
- Operation Mode
  - Router or NAT
- WAN connection method
  - Static IP, DHCP, PPPoE
- Dynamic DNS
  - Supported
- Network Time Protocol (NTP)
  - Sync built-in real-time-clock (RTC) with multiple external NTP servers
- IP Plug and Play (IP PnP)
  - Eliminate client IP reconfiguration
- DHCP modes
  - Act as DHCP server or relay
- IP/ Port Destination Redirection
  - 40 set of IP or Port address redirection

Manufacturer
OvisLink Corp.
2F, No. 8, Lane 130, Min-Chuan Rd, Hsin-Tien City, Taipei, Taiwan.

- SMTP Redirect
  - Support 1 Simple Mail Transmit Protocol redirection
- Specific Route
  - 6 sets of routing profiles with 10 rules each
- HTTP Proxy Server
  - 10 sets
- DMZ Server Mapping
  - 40 sets
- Virtual Server Mapping
  - 40 sets

User Management

- 2000 Instant Account (10 account Type)
- 500 Local User Account
- User Policy
  - 3 user policy (Firewall, routing profile, bandwidth control, login schedule, Black List)
- MAC ACL
  - 40 sets of MAC addresses which are allowed to open login page
- Authentication Method
  - POP3, POP3S, LDAP, RADIUS, Windows Domain Server
- POP3 Server Authentication
  - support SSL (POP3S
- LDAP Server Authentication
  - Server IP, Port Number , Base DN
- Windows Domain Server Authentication
  - Transparent login
- RADIUS Authentication
  - PAP/CHAP
- RADIUS Attributes
  - Start time,End time ,User ID, User MAC , User IP, Packets In,Bytes In, Packets Out, Bytes Out , User-Name, Calling-Station-Id, Framed-IP-Address, Acct-Terminate-Cause, Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets, Acct-Output-Packets
- WISP Support
  - GRIC
- Multiple Login on single account
  - Yes
- Privilege IP/MAC
  - 40 sets, no authentication required
- Session idle timeout
  - in minutes ; up to unlimited
- Login notification email
  - automatic POP3 email link to login page

Security Functions

- Firewall
- 3 sets of firewall profiles with 10 rules each based on Protocol/ Port/Source MAC/Source Port/DestinationPort/ SourceIP/DestinationIP/ network segment
- Walled Garden
- DoS Protection
- INMAP FIN/URG/PSH ; Xmas Tree; SYN/RST; Ping of Death; Null Scan; SYN/FIN
- User SSL web Login
- supported
- User Isolation Technology
- block communication between all downstream clients
- Secured Shell Host
- SSH Console login
- VPN pass-through
- IPSec and PPTP

Air Live®
Powered by OvisLink Corp.

Specification

Reporting / Monitoring

- Online User Monitoring
  - Reporting Field: ID, IP, MAC, Packet In/Out, Idle time, force logout
- Authentication Sever fail
  - Error message with admin contact info
- WAN Fail detection
  - Deny or open all access with error message
- Device monitoring
  - Monitor up to 40 IP devices alive status
- User History Log
  - Field: Start/End Time, ID, IP, MAC, Packet In/Out, Idle time
- History log email
  - Send out every 1~12 hr or stored up to 3 days

Accounting

- External Accounting Servers
  - RADIUS, Optional Micros-Fidelio Property Management System (PMS)
- Billing Plans
  - Up to 10
- Billing Method
  - Time (hour) or Network Usage (MB)
- Credit Redemption
  - customers add credit to account prior expiration
- RTC
  - built-in real time clock

System Administration

- SNMP support
  - SNMP V2c ready-only access
- SSH remote management
  - Supported
- 128bit SSL web admin
  - Supported
- Customized Login/logout page
  - Image limited at 512K
- Remote firmware update
  - Supported
- External Syslog Server
  - Supported
- Console admin functions
  - Reset / change admin password / debug utilities / service status
- Firmware backup/restore
  - Supported
- Remote firmware update
  - Web UI
- Console Admin
  - reset / change admin password / debug utilities / service status

Physical Specification

- Dimensions：239 mm x 156 mm x 30 mm
- Operating Temperature : 0 ˚C ~ 40 ˚C
- Storage Temperature: 0 ˚C ~ 60 ˚C
- Operating Humidity：10~80% non-condensing
- Storage Humidity: 5%~90% non-condensing

Ordering Information

MW-2000S Wireless Security Gateway

Manufacturer
OvisLink Corp.
2F, No. 8, Lane 130, Min-Chuan Rd, Hsin-Tien City, Taipei, Taiwan.